

SMTP Protocol and Its Security Vulnerability: Email Spoofing 1. Malware distribution across organizational networks. Mitigation Strategies To combat email spoofing, several technologies have been developed: SPF (Sender Policy Framework): Specifies authorized mail servers for a domain, helping detect forged sender addresses. Because traditional SMTP does not require sender verification, attackers can easily exploit this weakness to conduct phishing campaigns or spread malware. Case Study: Snapchat Email Spoofing Incident (2016) In 2016, Snapchat became a victim of a notable spoofing attack in which cybercriminals impersonated the company's CEO and successfully deceived an employee into sharing sensitive payroll data. This breach highlighted the real-world dangers of SMTP's lack of authentication and reinforced the importance of advanced email security protocols. DMARC (Domain-based Message Authentication, Reporting, and Conformance): Builds on SPF and DKIM to provide comprehensive policy enforcement and reporting. Retrieved from: <https://www.cisco.com/c/en/us/products/security/email-security/index.html> The Verge. Operating primarily on port 25, SMTP facilitates the reliable transmission of electronic messages across networks. Despite its widespread adoption, the original design of SMTP lacked robust authentication mechanisms, making it vulnerable to various attacks. Although modern implementations support encryption via SSL or TLS, the protocol still faces significant security challenges. References Cloudflare. 2.3.5. (2016).